HCLTech | Supercharging Progress™

Cybersecurity management and cyber resilience in financial services

Dr. Elif Kiesow Cortez &
Dr. Martijn Dekker

In partnership with

HSD The Hague Security Delta

Foreword

Dr. Martijn Dekker
CISO, ABN AMRO

Dr. Elif Kiesow Cortez
Research Fellow, Stanford University

Dear Readers,

We are glad to share with you our insights through this whitepaper on 'The Importance of Cybersecurity Management and Cyber Resilience in Financial Services'. We were able to gather valuable corporate views and practices during an exceptional time in the midst of the Covid-19 pandemic, where firms were confronted with radically changed circumstances. These exceptional times affected corporate work arrangements and communication due to the necessity of remote work and proved to be an immediate test for the readiness and agility of cybersecurity strategies of firms, and of financial companies in particular. Therefore, it was important to obtain the views of decisive company insiders, financial industry CISOs, on how they navigated this potential cybersecurity challenge. This whitepaper offers some of the major insights from this work and can provide lessons learnt that can inform future cybersecurity strategies and help them in their resilience and readiness for eventual future events of a disruptive nature.

Dear Readers,

We have seen outstanding work done in the last two years to manage cyber risks, evident in security investments and steps taken to improve cybersecurity. Recent reports suggest that the changes in organizational culture following the pandemic have intensified cybersecurity threats in the financial services (FS) sector. With internal actors in Financial Services contributing significantly to breaches, the resiliency approaches of FS organizations is in serious doubt. Resilience is a core theme of HCLTech's cybersecurity solutions. We believe that financial services organizations must build both defensive and offensive capabilities to achieve cyber-resilience.

Although we help leading financial services organizations address their cybersecurity concerns with our cybersecurity knowledge and domain expertise, we wanted to analyze the larger picture outside our clientele. It led us to form a collaboration with HSD and interview CISOs/CSOs to get their invaluable perspectives on cybersecurity. We have shared the insights collected during these interviews, including some key challenges they face and best practices they follow. We hope you find these insights helpful.

Sudip Lahiri,
Executive Vice President & Head – Europe, Financial Services, HCLTech

The importance of cybersecurity management and cyber resilience in financial services

The World Economic Forum recognizes that systemic cyber risk is one of the most probable and potentially impactful risks for firms.[1] While the pandemic significantly sped up the adoption of cloud and remote working technologies[2], the importance of cybersecurity was never in doubt amid a growing digital landscape for business. The advancements we have seen across industries have led to a proliferation of touch points and an inevitable transformation of the attack surface, with added complexity and interdependency across the digital supply chain.

Over the last few years, we have seen a substantial rise in cyber-attack events. The second quarter of 2022 alone saw around 52 million data breaches.[3]

It is no surprise that cybersecurity risks are increasing in number and growing in complexity for organizations worldwide. The financial sector in the Benelux region was already digitalizing fast, with recent remote working requirements further contributing to the new cybersecurity risk exposure in the financial sector. We interviewed 12 chief information security officers/chief security officers (CISOs/CSOs) from leading organizations from the financial sector in the Benelux region. We hereby present to you their views on the most pressing cybersecurity management issues in the financial sector.

Pressing cybersecurity concerns

The Verizon Data Breach Investigation Report 2022 shows that in the financial sector, 27% of the breaches are caused by internal actors.[4] The report also shows that miscellaneous erroneous actions are still the common cause for breaches as was the case previously. Since 2018, it is observed that threats by external actors are decreasing and threat by internal actors is on the rise and it is highlighted that this decrease and increase pattern occurs at a very similar rate.[5] In the public administration domain, majority threats are accounted for by personal data (46%) and credentials (34%). According to the IBM's Security Cost of Data Breach report 2022, the average cost of a breach increased 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022.[6]

According to Statista, during the third quarter of 2022, approximately 15 million data records were exposed worldwide through data breaches.[7] This figure had increased by 37 percent compared to the previous quarter. An increase in the number of attacks targeting the Microsoft Remote Desktop protocol was also reported. Moreover, the average cost of a ransomware attack was $4.54 million in 2022, which is slightly higher than the overall average total cost of a data breach, according to a recent study by the World Economic Forum.[8]

Organizations are vulnerable to private data leakages due to human-induced errors and misperception of risks. Addressing these vulnerabilities effectively is difficult and requires sustained commitment from management. Chatterjee and Sokol (2021) point out that firms spend much less on data breach-related compliance than on other traditional areas of compliance such as anti-bribery and audit fraud.[9]

ENISA's report shows that current prime threats include ransomware, malware, cryptojacking, e-mail-related threats, threats against data, threats against integrity and availability, disinformation, non-malicious threats and supply-chain attacks.[10] With regards to cybersecurity trends, the report also highlights how the last few years have seen the increasing role of state-sponsored actors through cyber espionage.[11] Threat actors such as hacker-for-hire actors are also targeting the financial services sector for purposes of corporate espionage.[12]

> It was reported that cyber-attacks targeted at the workforce significantly increased during remote working… and the company had to improve their awareness campaigns as hybrid working is becoming a standard.

From the eyes of the CISOs in financial services

For this research, we interviewed 12 CISOs/CSOs from top organizations in the financial sector in the Benelux region. As a part of the interview, we asked them on which tasks under cybersecurity risk management and cyber resilience do they spend most of their time daily. The following were their responses, in order of popularity:

Cybersecurity awareness trainings

Demonstrable operational effectiveness of cyber hygiene capabilities

Third-party risk management

Our respondents also emphasized various other cybersecurity challenges such as concerns about state-actor intrusion, the need for decentralizing security decision-making into DevOps teams and business alignment regarding implementation of cybersecurity practices in the full operation chain of the company.

The CISOs/CSOs in the interview panel were also asked about their current best practices in cybersecurity risk management and cyber resilience. The frequently reported best practices included communicating with senior management via applied examples of incidents from other financial sector firms, execution of security by design principles, sharing threat intelligence, a zero-trust approach and taking central decisions and explaining the reasoning behind certain security rules to the team(s).

When asked about the impact of recent years on cybersecurity best practices, several survey participants reported that hybrid working increased the importance of, and brought about a further focus on, acceleration. In our interviews, it was disclosed that after the last two years,

> It was disclosed that after the last two years, cybersecurity awareness in senior management increased and the risk appetite for cybersecurity decreased

cybersecurity awareness in senior management increased and the risk appetite for cybersecurity decreased. In line with the ENISA's threat landscape report,[13] our survey respondents reported that cyber-attacks targeted at the workforce significantly increased during the remote-working periods throughout the last two years. As a result, their respective companies had to improve their awareness campaigns as hybrid working is becoming a standard.

Our interviewees almost uniformly responded to the question about their financial institutions' future work model. Going forward, they expect remote working to become more prominent and the envisioned work model to remain hybrid. They envisage employees continuing to work from home and coming to the office when required in some instances.

A look into the future of cybersecurity management

When asked about which parameters are becoming increasingly important for cybersecurity management in financial services, our CISO/CSO participants responded that they expect the investments to increase in the domains of data integrity, data quality and operational effectiveness. Concomitantly, these areas have also received increased regulatory attention over the last two years.

The Financial Stability Board (FSB), the international body that monitors the global financial system, defines cyber resilience as a key element in their work program to promote financial stability. In their report for Effective Practices for Cyber Incident Response and Recovery, FSB advises that the boards should be in charge of the risk management strategy and should set achievable cyber incident response and recovery objectives to enhance cyber resilience in organizations.[14] In our

> Cybersecurity is more than an IT topic. Being cyber resilient is not only a quality of your IT estate, it is also a quality of your entire organization.

interviews, the CISOs/CSOs also highlighted that cyber resilience will be gaining more importance. Our participants emphasized that data recoverability became a top priority for cyber resilience practices in the financial sector. This was due to increased data breaches in recent years, both in terms of number and volume.

The comprehensive study of Jamilov et al. (2021) put forward several stylized facts on the emerging global cyber risk from analyzing the resulting indices including their time-trends.[15] The data in this study covers over 12,000 firms located in 85 countries spanning from 2002 until now at a quarterly frequency. Industrial composition of global cyber risk exposure is shifting toward the financial sector. The finance industry exhibited very little exposure before 2014. It is now the third most-affected sector after IT and Professional Services (the sector that includes the cyber-sensitive IT consulting firms) and before Manufacturing.

In our interviews, we also asked our participants what kind of changes they foresee encountering in their tasks in the next two to five years. The areas that they highlighted most frequently included:

01 The need for cybersecurity awareness and self-service capabilities by increasing consumability of security measures for each employee

02 A shift towards 100% coverage for security services, triggered by the further use of cloud environments

> It was understood that…cybersecurity is now seen as a business enabler also in light of the much more frequent uses of the cloud environments for collaborative working on sensitive documents.

Now that information security is recognized as an existential business risk, boards will expect CISOs to be more transparent about the security posture of the company. They will also expect CISOs to better articulate the security return on investments.

About Us

HCLTech is a global technology leader in the financial services industry. At HCLTech, we combine our deep domain expertise with technology capabilities to deliver digital, engineering, and cloud solutions to financial services enterprises. We lead the digital transformation initiatives of 5 out of the top 10 leading global investment banks, including the top 2 retail banks across each geography. Among our vast portfolio of technology solutions include Cybersecurity & GRC services, which aim at offering proactive, structured, and industry-relevant solutions to help banks defend their cyber infrastructure and achieve cyber resilience.

HCLTech's Cybersecurity & GRC Services is a 25+ years mature business practice focused on solving some of the most complex and most extensive cybersecurity challenges for 600+ customers globally. With a global network of 6000+ dedicated, certified professionals, 50+ Global Delivery Centers (GDCs), and six Cybersecurity Fusion Centers (CSFCs) across geographies, we can fast-track the cybersecurity transformation journey and drive expected business outcomes. Our Cybersecurity & GRC Services offers a Dynamic Cybersecurity Framework that provides a comprehensive service suite that hunts for threats across IT and OT attack surfaces, deploys purpose-built automation using AI/ML algorithms to contextualize business impact in real-time, and drives automated rapid response and recovery options.

To know more, connect with:

Prabhat Kumar
Sr. Director - Cybersecurity & GRC - EMEA Head, HCLTech
Mail: prabhat-kum@hcl.com

Deepak Arora
Vice President and Head of Banking for Europe, HCLTech
Mail: arorad@hcl.com

References

1. WEF, 2016. Understanding Systemic Cyber Risk. World Economic Forum: Global Agenda Council on Risk and Resilience, available at https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf.

2. WEF, 2021. Why the time has come to embrace the Zero-Trust model of cybersecurity. World Economic Forum, https://www.weforum.org/agenda/2021/10/why-the-time-has-come-for-the-zero-trust-model-of-cybersecurity/.

3. Statista Research Department. Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022. https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/#:~:text=Global%20number%20of%20breached%20data%20sets%202020%2D2022&text=During%20the%20third%20quarter%20of,compared%20to%20the%20previous%20quarter.

4. Verizon Data Breach Investigations Report 2022. Available at https://www.verizon.com/business/resources/reports/dbir/2022/public-administration-data-breaches/

5. ENISA 2022. Endnote:iv

6. 2022 IBM Security Cost of a Data Breach Report.

7. Statista Research Department. Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022. https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/#:~:text=Global%20number%20of%20breached%20data%20sets%202020%2D2022&text=During%20the%20third%20quarter%20of,compared%20to%20the%20previous%20quarter.

8. Lallie, H. S., L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers Security, 105.

9. Chatterjee, C. and D.D. Sokol, 2021. Data Security, Data Breaches, and Compliance. In: van Rooij, B. and D.D. Sokol (eds.) Cambridge Handbook on Compliance, Cambridge University Press: Cambridge, pp.936-948.

10. ENISA 2022. Endnote:iv

11. Ibid.

12. Kaspersky 2020. APT trends report Q3 2020. Available at https://securelist.com/apt-trends-report-q3-2020/99204/

13. ENISA 2022. Endnote:iv

14. Financial Stability Boards, Effective Practices for Cyber Incident Response and Recovery, 19 October 2020.

15. Jamilov, R., et al. 2021. Endnote:iii